Daily Open Source Infrastructure Report
25 April 2012

Top Stories

- Officials worked to place booms to stop oil from getting into waterways after a stubborn fire at a recycled oil refinery in Utah County, Utah. The refinery could be closed for a few months. – *KSL 5 Salt Lake City* (See item **4**)
- An internal audit found many U.S. Environmental Protection Agency radiation monitors were out of service at the height of the 2011 Fukushima power plant meltdown in Japan. – *Global Security Newswire* (See item **9**)
- Russian-speaking hackers earned about $4.5 billion globally in 2011, using various online criminal tactics targeting the financial sector and individual bank accounts, a new report found. – *IDG News Service* (See item **15**)
- Copper thieves cut a fiber optic cable, knocking out broadband service to thousands of customers, including two sheriff's stations, in the San Diego area April 24. – *KNSD 7 San Diego* (See item **52**)
- A 6-alarm fire ripped through the top floor of a condominium complex in Marlborough, Massachusetts, leaving 67 people temporarily homeless. The fire also closed area roads and a courthouse. – *Framingham MetroWest Daily News* (See item **54**)

Fast Jump Menu

Energy Sector

Current Electricity Sector Threat Alert Levels: Physical: LOW, Cyber: LOW
Scale: LOW, GUARDED, ELEVATED, HIGH, SEVERE [Source: ISAC for the Electricity Sector (ES-ISAC) - [http://www.esisac.com]

1. *April 24, Reuters* – (Louisiana; International) **US charges ex-BP engineer obstructed spill probe.** A former BP engineer was arrested and charged April 23 with trying to destroy evidence related to how much oil was spilling from the company's broken well in the Gulf of Mexico in April 2010, the U.S. Department of Justice said. He was accused of trying to delete text messages between him and a supervisor that included "sensitive internal BP information collected in real-time" as BP tried to stop the leak. The man was charged with two counts of obstruction of justice for allegedly deleting records related to the amount of oil flowing from the Macondo well after the blowout. The man, a drilling and completions engineer for BP before he resigned in January, worked on various efforts to stop the leak, including a "top kill" that involved pumping heavy mud into the ruptured well to try to push back the oil. Prosecutors alleged in an affidavit that in October 2010, when he learned his electronic files were going to be collected by a vendor working for BP's lawyers, he deleted hundreds of text messages about the top kill that indicated it was failing as top BP officials said publicly it was "broadly proceeding according to plan." Those deleted texts included one that said the well's flow rate was higher than BP scientists had said it would be if the top kill was working.
   Source: http://www.reuters.com/article/2012/04/24/bp-charges-idUSL2E8FOACZ20120424

2. *April 23, Government Computer News* – (National) **Smart-grid tech outpacing security, in 'delicate dance with risk'.** Development and deployment of smart-grid technology such as intelligent electric meters has outpaced security, setting up a "delicate dance with risk," according to the head of an industry advisory group, Government Computer News reported April 23. The head of the Energy Sector

Security Consortium (EnergySec), a non-profit forum for the exchange of security information among asset owners, industry partners, and the U.S. government, said installation of new equipment is already under way and slowing down to wait for security to catch up is not an option. He made his comments in the wake of a survey of energy industry security professionals in which large majorities of respondents said that security controls and standards are not keeping pace with the rollout of new equipment.
Source: http://gcn.com/articles/2012/04/23/smart-grid-tech-outpaces-security-hacker-opportunity.aspx

3. *April 23, United Press International* – (Pennsylvania; New York; National) **Spring snowstorm blankets parts of northeast.** A rare spring snowstorm blanketed parts of the northeast and cut off power to more than 75,000 customers in Pennsylvania and upstate New York, officials said. By April 23, 6 inches of snow had fallen in higher elevations of Pennsylvania, with 12 inches reported in certain areas. MSNBC reported snow was falling in upstate New York, West Virginia, Maryland, and Pennsylvania, with the heaviest snowfall at a rate of more than 1 inch per hour. Winter storm warnings were in effect from the higher elevations of West Virginia northward to western New York state, the National Weather Service said. Winter weather advisories were in effect for the Adirondacks in New York and in northern Maine, while flood watches were in effect for parts of eastern New York, and parts of New Hampshire and Maine.
Source: http://www.disasternews.net/news/article.php?articleid=4592

4. *April 23, KSL 5 Salt Lake City* – (Utah) **Officials investigating dangerous oil refinery fire.** Federal, state, and local investigators and specialists are looking further into a fire at a recycled oil refinery in Utah County, Utah, the week of April 16. The fire shut down the plant and had crews scrambling to place booms in Utah Lake over fears of where the oil might go. The fire took place April 19 in an oil tank at Rock Canyon Oil in American Fork. It re-ignited a half-dozen times, the company general manager said. The firm believes the problem may have been a crack in a tube used to heat the oil tank, though the official cause has not been determined. April 20, officials with the Utah Department of Environmental Quality and Occupational Safety and Health Administration joined the Utah County Fire Marshal and city sewer workers in surveying the site. The refinery could be closed for a few months. According to a spokesman, tens of thousands of dollars of fire equipment was damaged or ruined by the fire. Rock Canyon Oil did not have a damage estimate yet, according to the general manager.
Source: http://www.ksl.com/?nid=148&sid=20116565

5. *April 22, WGMD 92.7 Rehoboth Beach* – (Delaware) **Crews work to clean up diesel fuel spill at Port of Wilmington.** April 22, approximately 1,300 gallons of diesel fuel leaked from a storage tank of one of the Port of Wilmington, Delaware crane's onto the terminal and into a portion of Christina River adjacent to the Port's Berth 3 and Berth 4. The port's emergency response contractor responded to conduct spill containment and clean-up operations. Those operations continued throughout the day. The spill appeared to have been caused by an electrical malfunction of a fuel tank fill pump. Crane engineers were on the scene to further identify and correct the cause of this spill.

In the interim, no further leakage from the unit was anticipated. Port operations continued while the clean-up operations were in progress.
Source: http://www.wgmd.com/?p=54577

6. *April 20, Bloomberg* – (New Jersey) **Hess sued by U.S., N.J. over air emissions at oil refinery.** Hess Corp. was sued by the U.S. and New Jersey governments over air emissions at its petroleum refinery in Port Reading, New Jersey, and was expected to settle the case April 20, a Justice Department spokesman said. Hess violated federal and state laws in making a "major modification" to the refinery that resulted in a "significant net emissions increase" of nitrous oxide, sulfur dioxide, carbon monoxide, and particulates, according to the complaint filed April 19 in federal court. The refinery, which has a crude oil capacity of 65,000 barrels a day, was cited for violations at a fluid catalytic cracking unit catalyst regenerator, a sulfur recovery plant, and at flaring devices, heaters, and boilers, the complaint said. New York-based Hess failed to operate the facilities in a "manner consistent with good air pollution control practice" and also failed to comply with benzene waste requirements, officials said. The complaint, by the U.S. Justice Department's environmental and natural resources division and the New Jersey attorney general, seeks civil penalties of as much as $37,500 a day for the various violations.
Source: http://www.bloomberg.com/news/2012-04-20/hess-sued-by-u-s-n-j-over-air-emissions-at-oil-refinery-1-.html

For another story, see item **18**

[Return to top]

Chemical Industry Sector

7. *April 24, Central Florida News 13 Orlando* – (Florida) **Truck crash spills sulfuric acid on Polk highway.** A flatbed truck carrying 1,000 gallons of sulfuric acid spilled onto a Bartow, Florida highway, forcing the closure of a busy stretch of road for at least 6 hours, April 24. According to a Polk County spokesman, the driver performed a hard stop, causing the truck to overturn, spilling several containers of acid onto State Road 60 near Rifle Range Road. Officials said the driver was burned by the acid. He was airlifted to a local hospital. Both State Road 60 and Rifle Range Road were closed in all directions near the spill. A HAZMAT team responded. The flatbed truck that crashed was also carrying salt pellets, which are used in water filtration. When those pellets mix with sulfuric acid, it results in hydrogen chloride gas. The hazardous materials spilled in the crash can cause respiratory problems. Polk County officials sent out a reverse 9-1-1 call to inform residents about the situation. Officials advised those in the general area there was a potential for fumes and that they should shut windows and turn off air conditioners.
Source:
http://www.cfnews13.com/content/news/cfnews13/news/article.html/content/news/articles/bn9/2012/4/24/tanker_truck_crash_s.html

8. *April 23, Baltimore Sun* – (Maryland) **Caustic acids stored inside warehouse, site of three-alarm Canton blaze.** With a warehouse fire in the Canton section of Baltimore reduced to a smolder by April 23, attention shifted to ensuring surrounding homes and the harbor's waters were protected from caustic chemicals. State and federal environmental officials were on site alongside firefighters late into April 23, monitoring water streaming from the one-story brick structure into storm drains and the harbor at the Canton waterfront. The warehouse contains nearly 8,000 gallons of corrosive chemicals, including sodium hydroxide, a powerful base, and sulfuric, nitric, and chloric acids, a Maryland Department of the Environment (MDE) spokesman said. He said no dangerous levels of acid were detected. Warehouse owner Eastern Plating anodizes metals. Eastern has hired an environmental contractor to help it remove chemicals from the rubble, the MDE spokesman said. About 90 firefighters responded to the 3-alarm blaze April 22 and evacuated 60 nearby residents. Most of the roof collapsed, and the small brick facility was condemned. When firefighters responded, they were not aware of any chemicals inside the building, a city fire chief said. Businesses are required to publicly post any chemicals they use or store, but because the building was in flames, that information was not available, he said. The chief noted that fire officials were able to contact the company's owner as firefighters tackled the blaze.
   Source: http://articles.baltimoresun.com/2012-04-23/news/bs-md-warehouse-fire-canton-20120423_1_chemicals-storm-drains-firefighters

For more stories, see items **4**, **6**, and **56**

[Return to top]

Nuclear Reactors, Materials and Waste Sector

9. *April 23, Global Security Newswire* – (National) **Audit confirms EPA radiation monitors broken during Fukushima crisis.** An internal audit confirmed observers' concerns that many of the U.S. Environmental Protection Agency's (EPA) radiation monitors were out of service at the height of the 2011 Fukushima power plant meltdown in Japan, Government Security Newswire reported April 23. The report detailed problems with the agency's "RadNet" monitoring system. Agency contractors are responsible for maintaining the monitors and repairing them when they are broken. However, according to the report, the EPA has not managed those contracts as high priorities, despite having identified the monitors as "critical infrastructure" under the 2001 Patriot Act. As a result, there have been numerous delays in repairing broken monitors. In addition, the agency has in many instances allowed filters to go unchanged for longer than the twice-per week that its policy dictates, the audit said. Because of these issues, 20 percent of the monitors were out of service the day the Fukushima crisis began, according to the report.
   Source: http://www.nti.org/gsn/article/audit-confirms-epa-radiation-monitors-broken-during-fukushima-crisis/

[Return to top]

Critical Manufacturing Sector

10. *April 24, Daily Tech* – (International) **Nissan gets hacked, target could've been intellectual property.** Nissan Motor Company announced that its information systems were hacked, Daily Tech reported April 24. The company did not know who the hackers were or where they struck from, and it was unclear what data may have been compromised. Nissan believes the hackers were looking for intellectual property related to its EV drivetrains. Nissan maintained it quickly secured its system and issued a statement alerting customers and employees that its data systems were breached. Nissan said the infiltration was noticed April 13. A Nissan statement said the company's security team confirmed the presence of a computer virus on their network, and took action to protect systems and data.
    Source: http://www.dailytech.com/Nissan+Gets+Hacked+Target+Couldve+Been+Intellectual+Property/article24527.htm

11. *April 24, Detroit News* – (International) **Carmakers OK plan to speed resin substitute.** A group of major automakers agreed April 23 to a process to speed the use of alternative materials in place of a key resin that may soon be in short supply. Supply of the resin, PA-12 or nylon-12, was jeopardized after a late March explosion at an Evonik Industries AG chemical plant in Marl, Germany. The resin is used by automakers in coatings and fuel and brake systems. The group of 6 major automakers and 19 suppliers drafted a plan to hasten approval of alternatives to PA-12, according to an e-mail statement from the Automotive Industry Action Group, a nonprofit that works with automotive companies.
    Source: http://www.detroitnews.com/article/20120424/AUTO01/204240355/Carmakers-OK-plan-speed-resin-substitute?odyssey=mod|newswell|text|FRONTPAGE|p

12. *April 23, Austin Post-Bulletin* – (Minnesota) **Fire damages fabricating plant.** Smoke damage from an electrical fire April 22 was expected to close Kappers Fabricating in Spring Valley, Minnesota, until it can be repaired. The electrical room was destroyed and will need to be rewired. Elsewhere in the steel building, smoke damage was extensive. There was no damage estimate, but damage to the computers and other equipment that control the metal fabrication could be extensive, according to a local fire chief.
    Source: http://www.postbulletin.com/news/stories/display.php?id=1494080

[Return to top]

Defense Industrial Base Sector

Nothing to report

[Return to top]

Banking and Finance Sector

13. *April 24, Help Net Security* – (International) **Phishing and malware meet check fraud.** Trusteer recently uncovered a scam in an underground forum that shows how data obtained through phishing and malware attacks can be used to make one of the oldest forms of fraud — check forging — even harder to prevent. The scam involves a criminal selling pre-printed checks linked to corporate bank accounts in the United States, the United Kingdom, and China. The criminal is selling falsified bank checks made with specialized printing equipment, ink, and paper. For $5 each, they will supply checks that use stolen data provided by the buyer. However, to purchase checks that use stolen credentials supplied by the counterfeiter the cost is $50. Check data fields include personal information and financial data. To obtain all the required data, fraudsters typically must get their hands on a physical or scanned version of a real check in circulation. Many banking Web sites provide access to scanned versions of paid and received checks. Online banking log-in credentials obtained through malware and phishing attacks can be used to access a victim's account and collect all the required information to commit check fraud. Also, before using the checks, fraudsters can ensure account balance is sufficient to approve the transaction. The criminal recommends using the checks to buy products in stores rather than trying to redeem them for cash. Buyers are encouraged to carry fake identification cards that match stolen credentials on the check. The check counterfeiter offers to provide these too.
    Source: http://www.net-security.org/secworld.php?id=12793

14. *April 24, Associated Press* – (Pennsylvania; Florida) **More than $1M found in armored car heist arrest.** Between $1.3 million to $1.5 million of the money that a man allegedly stole from the armored car he was working on has been recovered, along with the gun likely used to kill his co-worker in Pittsburgh, an FBI special agent said April 24. The special agent in charge, who heads the Pittsburgh FBI office, told reporters April 24 that the suspect led investigators to the money, which was part of the $2.3 million that went missing from the armored car he was paid to guard. The agent also said the suspect, who was being cooperative, had a pair of handguns with him when he was arrested in Florida, including the one supplied by his company, Garda Cash Logistics. He said the suspect had "indicated" that was the weapon used in the shooting and robbery.
    Source: http://www.foxnews.com/us/2012/04/24/pittsburgh-armored-car-slay-suspect-nabbed-in-fla/

15. *April 24, IDG News Service* – (International) **Russian cybercriminals earned $4.5 billion in 2011.** Russian-speaking hackers earned an estimated $4.5 billion globally using various online criminal tactics and are thus responsible for 36 percent of the estimated total of $12.5 billion earned by cybercriminals in 2011, Russian security analyst firm Group-IB said in a report published April 24. The researchers estimate the total share of the Russian cybercrime market alone doubled to $2.3 billion, while the whole Russian-speaking segment of the global cybercrime market almost doubled, to $4.5 billion. In 2011, the cybercrime market was embraced by traditional organized crime groups trying to control the entire theft process. The cybercrime market has consolidated, with the rise of several major groups. This could lead to "an explosive

increase of attacks" on the financial sector, the researchers warned. Online banking fraud, phishing attacks, and the theft of stolen funds increased within Russia and was the largest area of cybercrime, amounting to an estimated $942 million. In Russia, there also was a trend in targeting individuals rather than financial institutions for online banking fraud, and criminals mainly used Web-inject technologies and trojan programs to lead users to phishing sites.
Source:
http://www.computerworld.com/s/article/9226498/Russian_cybercriminals_earned_4.5_billion_in_2011

16. *April 23, Help Net Security* – (National; International) **Bank of America phishing emails doing rounds.** Fake warning e-mails are targeting Bank of America customers and asking them to update their account. With "Bank of America Warning : Error Statement" in the subject line, the vaguely credible HTML e-mail states the target's "Bank of America account showed unusual activities this morning." "What to do next? Sign in now to verify your logon details," the e-mail urges. Unfortunately, all the links in the e-mail take the recipient to a spoofed Bank of America Web site, where they are asked to sign in by entering their log-in details and are prompted to share additional personal and financial information to "verify" their accounts. "The care and detail with which the scam email has been created makes this phishing scam attempt a little more sophisticated than some other such attacks and may fool at least a few bank customers into supplying the requested details," according to Hoax-Slayer.
Source: http://www.net-security.org/secworld.php?id=12788

17. *April 23, Associated Press* – (New York) **NY attorney general files fraud suit against company that leases credit card machines.** The New York attorney general (AG) April 23 sued a company that leases credit card machines to small businesses, claiming Northern Leasing Systems Inc. fraudulently attempted to drain more than $10 million from 100,000 former customers with expired leases. The AG's office said the firm kept at least $3.5 million from the scheme launched in March 2011, while disguising it with a shell company called SKS Associates LLC. The complaint also names Northern Leasing affiliates Lease Finance Group LLC, MBF Leasing LLC, Golden Eagle Leasing LLC, and Lease Source-LSI LLC all operating from the same address. The lawsuit seeks restitution, disgorgement of profits, penalties, and fees. The AG said the investigation was prompted by more than 70 complaints, and the firm claimed it was collecting taxes and administrative fees previously unpaid. The suit cited two class-action lawsuits and hundreds of complaints against Northern Leasing alleging predatory sales and deceptive lease agreements. Leases typically had 4-year terms with automatic monthly payments that required customers to provide checking account and bank routing numbers. "Ultimately, over 77 percent of the amounts sought by SKS were not even taxes at all but merely alleged 'fees' related to the taxes," the complaint said. "Respondents debited former customers with expired contracts, including many customers who had received releases from their contracts when they executed buyout options to purchase the equipment."
Source:
http://www.therepublic.com/view/story/a816eb2e1bfa44f5b657b8f4ae3f5bea/NY--Leasing-Company-Sued/

18. *April 23, Reuters* – (Louisiana; National; International) **SEC charges SinoTech, execs.** Securities regulators charged China-based SinoTech Energy Ltd. and its senior executives with misleading investors April 23, part of an effort to crack down on accounting problems at Chinese companies listed in the United States. The U.S. Securities and Exchange Commission's (SEC) civil suit, filed in a U.S. district court in Louisiana, alleges the oil field services company and its executives "continuously and intentionally misled investors" about the value of its assets and how it used the $120 million in proceeds from its November 2010 initial public offering. The SEC alleges SinoTech's chief executive officer and former chief financial officer were responsible for the fraud. The SEC also charged the company's chairman, saying he stole $40 million from a SinoTech bank account. The investor protection agency is seeking financial penalties and to bar the executives from serving as officers or directors of U.S. public companies. SinoTech was previously listed on the Nasdaq market, but its shares were halted in August 2011, the SEC said. Nasdaq then suspended trading in October 2011, and delisted the stock January 6.
Source: http://www.reuters.com/article/2012/04/23/us-sec-sinotech-idUSBRE83M1EN20120423

19. *April 23, U.S. Securities and Exchange Commission* – (California) **SEC charges former CalPERS CEO and friend with falsifying letters in $20 million placement agent fee scheme.** The U.S. Securities and Exchange Commission April 23 charged the former chief executive officer (CEO) of the California Public Employees' Retirement System (CalPERS) and his close personal friend with scheming to defraud an investment firm into paying $20 million in fees to the friend's placement agent firms. The SEC alleges the two fabricated documents given to New York-based private equity firm Apollo Global Management. Those documents gave Apollo the false impression CalPERS had reviewed and signed placement agent fee disclosure letters in accordance with its established procedures. In fact, the pair intentionally bypassed those procedures to induce Apollo to pay placement agent fees to the friend's firms. The false letters bearing a fake CalPERS logo and the CEO's signature were provided to Apollo, which then went ahead with the payments. Based on these false documents, Apollo was induced to pay more than $20 million in placement agent fees it would not have paid without the disclosure letters.
Source: http://www.sec.gov/news/press/2012/2012-73.htm

[Return to top]

Transportation Sector

20. *April 23, Minnestoa Public Radio* – (New York) **Flight makes emergency landing; students OK.** A Delta Air Lines flight headed to Minneapolis and carrying students from Southwest High School in Minneapolis, made an emergency landing April 22 at John F. Kennedy International Airport in New York. A Delta spokesman said the plane took off from LaGuardia Airport in Queens, New York, April 22 and made an emergency landing when crew members detected an electrical smell. The emergency landing was precautionary, officials said. The flight landed without incident. The 145 passengers, including high school students and chaperones, were booked on a later

flight to Minnesota.
Source: http://minnesota.publicradio.org/display/web/2012/04/23/delta-flight-emergency-landing/

21. *April 23, Washington Post* – (Washington, D.C.) **Metro bus driver has viral meningitis; agency warns riders, employees.** Washington Metropolitan Area Transit Authority (Metro) said a bus operator on its 14th Street Line was diagnosed with viral meningitis, the Washington Post reported April 23. The bus operator last drove April 20, when he drove on the 52 and 54 routes of the Washington, D.C.-based transit system. The bus has been removed from service until it can be "thoroughly sanitized," Metro said. In addition, Metro said it would disinfect all 164 buses at its Northern Division. A Metro spokesman said the driver was diagnosed April 20. Before that day, the driver was on vacation and not driving a bus. Viral meningitis, according to the Centers for Disease Control, is "generally less severe and resolves without specific treatment," Metro wrote in a press release. The symptoms of viral meningitis usually last 7 to 10 days.
Source: http://www.washingtonpost.com/blogs/dr-gridlock/post/metro-bus-driver-has-viral-meningitis-agency-warns-riders-employees/2012/04/23/gIQAIRbncT_blog.html

For more stories, see items **7** and **54**

[Return to top]

Postal and Shipping Sector

22. *April 23, KOLN 10 Lincoln; KGIN 11 Grand Island* – (Nebraska) **Two men cited for vandalism spree.** A group of young men went on an extensive vandalism spree in Nebraska, causing thousands of dollars in damage, but they were cited then released by police. The incidents happened April 22. In total, there were 11 reports of vandalism, mostly to cars and two mailboxes. The total damage was estimated at $2,000. Police caught two of the three men they believe are responsible for the vandalism and officers are still searching for a third suspect.
Source:
http://www.1011now.com/home/headlines/Two_Men_Cited_for_Vandalism_Spree_148595985.html

[Return to top]

Agriculture and Food Sector

23. *April 24, Food Safety News* – (National) **USDA tightens rules for drug residues in food animals.** Federal meat safety officials are stepping up efforts to prevent meat with illegal levels of drugs or other chemicals from entering the food supply. The new plan — unveiled April 23 by the U.S. Department of Agriculture's Food Safety and Inspection Service (FSIS) — is two-pronged. First, the agency will release a new compliance guide for slaughter establishments outlining measures that can reduce or prevent residues in livestock. FSIS will also increase residue testing at establishments

with a record of residue violations, the agency said. This will protect meat containing residues from entering the food supply, and also will give past violators an incentive to use methods that do not produce illegal residue amounts. If cows were administered antibiotics, anti-inflammatory medicines, or other drugs, different withdrawal times, depending on the drugs, must elapse before they may be slaughtered and marketed. Culled cows that contain drug residues are not supposed to be sold to slaughterhouses nor is meat from animals with drug residues to be shipped into commerce. The new guidance is intended especially for establishments that slaughter dairy cows or bob veal calves, since these operations commit the majority of residue violations. FSIS also announced it is revamping its Residue Repeat Violator List — maintained by the National Residue Program — to make it "streamlined and more user-friendly."
Source: http://www.foodsafetynews.com/2012/04/usda-strengthens-prevention-of-residues-in-food-animals/

24. *April 23, Food Safety News* – (National) **Pathogen test rapidly hones in on Salmonella.** A new method of testing for Salmonella could shorten the time it takes to detect the bacteria in food samples, Food Safety News reported April 23. Researchers at the Agricultural Research Service's Quality and Safety Assessment Unit in Athens, Georgia, are using a technique called surface-enhanced Raman scattering (SERS), in which light from a laser is directed at a sample specimen, whose interaction with the light produces a unique spectral pattern called a "Raman spectral signature." Scientists postulate that each strain of bacteria has its own unique signature that acts as a badge of identity. Currently, bacteria are most often identified by their DNA fingerprint using pulsed-field gel electrophoresis (PFGE). These PFGE patterns are then uploaded onto PulseNet, a national database that can be used to see if the strain matches others in the system. However, PFGE analysis usually takes at least 24 hours to complete in a lab, whereas a test using SERS takes less than 30 minutes from start to finish, according to the lead researcher. He said if SERS proves effective, a worldwide Internet database could be created using Raman spectral signatures to find a match for bacteria more quickly, which could help investigators pinpoint the source of contamination earlier in an outbreak.
Source: http://www.foodsafetynews.com/2012/04/pathogen-test-rapidly-hones-in-on-salmonella/

25. *April 23, U.S. Department of Labor* – (Ohio) **U.S. Department of Labor's OSHA cites American Foods Group with 7 safety violations at Sharonville, Ohio, plant.** The U.S. Department of Labor's Occupational Safety and Health Administration (OSHA) cited American Foods Group LLC with seven safety violations — including one repeat — at the company's Sharonville, Ohio meat processing facility following a February 23 inspection conducted under OSHA's National Emphasis Program on Amputations. Proposed penalties total $47,000, said the April 23 U.S. Department of Labor statement. The repeat violation was failing to conduct periodic and regular inspections of lockout procedures for energy sources of equipment. Six serious violations involved failing to: train employees who service equipment so they were authorized to implement the energy control program; train employees on how to troubleshoot electrical equipment using safe work practices; train employees on the operation of powered industrial trucks; affix locks to energy isolation devices prior to

allowing employees to perform maintenance and servicing operations; and provide locks to production employees who service equipment. One other-than-serious violation was for failing to develop and implement energy control procedures for newly installed equipment that uses the same energy sources as other machines within the facility.
Source:
http://www.osha.gov/pls/oshaweb/owadisp.show_document?p_table=NEWS_RELEASES&p_id=22206

26. *April 23, U.S. Department of Labor* – (Wisconsin) **U.S. Department of Labor's OSHA cites Spurgeon Vineyards and Winery in Highland, Wis., with 12 violations including lack of guarding and training.** The U.S. Department of Labor's Occupational Safety and Health Administration (OSHA) cited Spurgeon Vineyards and Winery LLC in Highland, Wisconsin, with 12 safety and health — including nine repeat — violations for failing to provide fall protection and a hazard communication program. The citations were the result of a follow-up investigation conducted in January, the U.S. Department of Labor reported April 23. Proposed penalties totaled $71,280. Seven repeat safety violations involved failing to protect workers from fall hazards greater than 4 feet on wine tanks and catwalks, implement and train workers on a lockout/tagout program to control the release of hazardous energy, possess proper guarding and interlocks on a wine bottling machine, and to provide forklift training, as well as for allowing workers to use damaged electrical cords. Additionally, the company was cited with repeat health violations for failing to implement a personal protective equipment hazard assessment, provide a hazard communication program and training, and provide material safety data sheets for chemicals used in the workplace. Three serious safety and health violations cited included the operation of forklifts under lights without proper head room, a lack of eye protection, and failing to evaluate the risk of ozone exposure.
Source:
http://www.osha.gov/pls/oshaweb/owadisp.show_document?p_table=NEWS_RELEASES&p_id=22212

[Return to top]

Water Sector

27. *April 24, Beaver County Times* – (Pennsylvania) **Aliquippa water authority: Water back for everyone.** The Municipal Water Authority of Aliquippa, Pennsylvania, said water service was restored to its customers April 23, although a boil advisory remained in effect for most of the day. The authority's general manager said crews bled the system of air that accumulated as its workers repaired two main breaks in the city April 19 and 20. Those efforts delayed the restoration of service to the area and meant a drastic drop in water pressure for authority customers in Potter and Raccoon townships April 22.
Source: http://www.timesonline.com/news/local_news/aliquippa-water-authority-water-back-for-everyone/article_1a463167-2526-507d-b64f-a25370cdb26e.html

28. *April 24, WTOK 11 Meridian* – (Mississippi) **Boil water advisory for Northwest Kemper.** The Mississippi State Department of Health (MSDH) received an alert from the Northwest Kemper Water Association #4 in Kemper County April 24 of water pressure loss due to one or more line breaks. This affected about 286 customers on the Hwy 16 system. The MSDH initiated a boil water advisory until further notice.
Source: http://www.wtok.com/news/headlines/Boil_Water_Advisory_for_Northwest_Kemper_148694745.html?ref=745

29. *April 23, San Antonio Express News* – (Texas) **Electrical fire erupts at SAWS facility.** An electrical fire erupted for the second time in 2012 at a San Antonio Water System (SAWS) treatment facility April 23. SAWS officials said they did not expect any interruption in service. The fire battalion chief said an electrical panel inside a wall of SAWS' Basin Station caught fire. The small fire was controlled in less than an hour, and no chlorine leaks were found, though a HAZMAT crew was checking the area. No one was inside when the fire erupted because crews were working on repairs from another electrical fire that happened in January 2012. Officials did not know when the facility would be reopened, and said employees were still evaluating damage. Damage from January's fire was estimated at $100,000.
Source: http://www.mysanantonio.com/news/local_news/article/Electrical-fire-erupts-at-SAWS-facility-3502551.php

30. *April 23, El Centro Imperial Valley Press* – (California) **E. coli effluent violations alleged.** The pursuit of a settlement discussion with the California Regional Water Quality Control Board over alleged E. coli effluent violations was approved by the Holtville, California, City Council April 17. There were five effluent limit violations over the 2011 winter, said the waterworks supervisor. Holtville had a cease and desist order from the water board over ammonia discharges, and if they are not reduced by 2014 the state will fine the city. The violations pose no threat to human health; still, a penalty of $6,000 has been issued to the city, according to a report to the council. The council decided to engage the water board and ask it to apply those fines toward the improvements of the wastewater plant. The total cost of the wastewater treatment plant rehabilitation project is about $7.5 million.
Source: http://www.ivpressonline.com/news/ivp-e-coli-effluent-violations-alleged-20120423,0,419794.story

For more stories, see items **1**, **4**, **5**, and **8**

[Return to top]

Public Health and Healthcare Sector

31. *April 23, Insurance Journal* – (Florida) **Florida massage therapist, 14 patients charged with insurance fraud.** The Insurance Journal reported April 23 that Florida officials said they arrested a licensed massage therapist, a physician's assistant, and 14 massage clinic patients on charges of insurance fraud and grand theft as part of an undercover sting. Officials said the owner of Flamingo Health Corp. in Miami

allegedly billed insurance companies nearly $250,000 in fraudulent insurance claims and coached patients on how to commit personal injury protection fraud. The investigation determined the clinic owner directed undercover officers posing as patients to sign blank treatment forms and coached them on how to answer questions from their insurance company. The Florida Division of Insurance Fraud (DIF) and the Miami-Dade Police Department Public Corruption Investigations Bureau conducted the investigation. Additionally, the DIF was assisted by the U.S. Secret Service during the execution of a search warrant at Flamingo Health Corp.
Source: http://www.insurancejournal.com/news/southeast/2012/04/23/244429.htm

32. *April 23, Houston Chronicle* – (Texas) **Accused serial thief infiltrates dozens of hospitals, clinics in Houston.** Disguised as a nurse wearing scrubs, a serial thief managed to infiltrate dozens of hospitals and clinics around Houston, to steal purses and credit cards. "She's just walking into these hospitals uncontested," said a lieutenant from the Harris County Sheriff's Office. Once inside a hospital or clinic, she "cruises" around to find unmanned purses and then swiftly hits the stores. Investigators linked her to dozens of hospital thefts dating to February 2012. Her latest hit was April 20 at TOPS Specialty Hospital. Wearing scrubs, she slipped in through a back door, but was confronted and questioned by hospital administrators. She convinced them she left her identification in the car, and as she exited, managed to steal another nurse's purse. Authorities asked hospital workers to be on the lookout.
Source: http://www.chron.com/news/houston-texas/article/Accused-serial-thief-infiltrates-dozens-of-3503657.php#photo-2851289

33. *April 20, University of Arkansas Medical Sciences* – (Arkansas) **UAMS investigating breach of information.** The University of Arkansas for Medical Sciences (UAMS) discovered a breach of patient data, which resulted when a document sent to an individual outside of UAMS for analysis of billing was not properly de-identified. A UAMS physician sent the data to a person who was not a member of UAMS's workforce in mid-February 2012, with the intention of removing all patient identifiers. April 6, UAMS discovered the data did in fact contain identifiers, including patient names, UAMS account numbers, dates of service, interventional radiology procedures, diagnosis codes, and charges and payments, for about 7,000 patients. Patients affected were interventional radiology patients seen at UAMS from 2009-2011. No credit card, debit card, bank account, or Social Security numbers were included. UAMS contacted the recipient of the data, and was assured he had not disclosed the information to anyone else and that he did not look at or use patient names when he worked on his financial analysis. UAMS did discover the data was transmitted via a Web-based e-mail service, which a UAMS IT security officer determined to be a moderate risk. UAMS IT security worked with the recipient to ensure the information was permanently destroyed and no longer at risk. The UAMS employee who failed to properly de-identify the data has been placed in the disciplinary process for violating UAMS policies. UAMS also is conducting additional training of its workforce and evaluating policies to prevent an incident like this from recurring.
Source:
http://www.uamshealth.com/News/UAMSInvestigatingBreachofInformation?id=5349&showBack=true&PageIndex=0&cid=4

For another story, see item **35**

[Return to top]

Government Facilities Sector

34. *April 24, Detroit Free Press* – (Michigan) **Hartland High School closed after death threat discovered; police questioning suspect.** Investigators in Livingston County, Michigan, said they determined who spray painted a scrawling threat to shoot multiple people, closing Hartland High School in Hartland, April 24. The sheriff said April 24 that detectives were questioning a suspect. The Hartland Schools superintendent decided to close the school after officials found graffiti in the pool area and vandalism inside Hartland High School. She said the discovery set off a social media panic among students and parents late April 23. All activities at the school and pool area were cancelled April 24, according to the Hartland Consolidated Schools Web site. The sheriff said investigators were trying to determine whether the suspect acted alone.
Source: http://www.freep.com/article/20120424/NEWS06/120424009/Hartland-High-shut-down-today-after-death-threats?odyssey=tab|topnews|text|FRONTPAGE

35. *April 23, Gainesville Sun* – (Florida) **Chickenpox outbreak reaches 78 cases.** The largest outbreak of chickenpox in recent Alachua County, Florida, history hit 78 April 23 — and 1 of the cases had health officials closely watching Santa Fe High School, where 139 students have not been vaccinated against the virus. The volume of chickenpox cases concentrated in the northwest part of the county spawned an official effort to control the outbreak. The health department excluded dozens of unvaccinated students from class in March and April. One of the four new cases reported April 23 was at Santa Fe High School — the school's first case. With 139 students at the 1,129-student school not vaccinated against chickenpox, the health department director said he was going to make the vaccine available at school starting April 23. He said about 50 students at the school have been vaccinated since the outbreak. Students can come to school without a full set of vaccinations if they have either a religious or medical exemption from the requirement. However, the county has been flagged at the state level for its low level of students coming to school fully vaccinated. The director would not rule out taking more action to control the transmission of chickenpox at Santa Fe High School.
Source: http://www.gainesville.com/article/20120423/ARTICLES/120429834?tc=ar

36. *April 23, Boston Globe* – (Massachusetts) **Bomb threat, rainy weather combine to close Lincoln-Sudbury Regional High School.** Students at Lincoln-Sudbury Regional High School in Sudbury, Massachusetts, were dismissed from school early April 23 after an administrator discovered a bomb threat on an answering machine, school officials said. "Because a full sweep of the building is necessary to ensure the safety of all, and because the weather does not permit a lengthy wait outside the building, we have decided to call the buses and dismiss all students for the remainder of the day," the superintendent and principal said in an e-mail to parents. The message was left on a school answering machine over the weekend of April 21, according to the e-mail. Buses were called to pick up the students and bring them home.

Source: http://www.boston.com/Boston/metrodesk/2012/04/bomb-threat-rainy-weather-combine-close-lincoln-regional-sudbury-high-school/fylaEDqm9a8qcBta5m2fUO/index.html

37. *April 23, CNN* – (Washington D.C.) **76 arrested in Capitol protest over Medicaid cuts.** Seventy-six people were arrested April 23 at a demonstration in Washington D.C. protesting proposed cuts in Medicaid, authorities said. Hundreds of demonstrators filled the rotunda of the Cannon House Office Building. The 76 were arrested on suspicion of unlawful conduct and demonstrating in a Capitol building, police said. Police said most of those arrested would face a misdemeanor fine and be released after processing.
Source: http://www.cnn.com/2012/04/23/us/medicaid-protest/index.html?hpt=us_c2

38. *April 23, Associated Press* – (California) **California college resumes class after attack.** Some students at a California Christian college returned to class April 23 in a building where seven people were killed earlier in April. Oakland's Oikos University held a single class 3 weeks after police said a nursing student fatally shot 6 of his fellow students and a receptionist. The small school had been busy preparing to resume operations by replacing carpet and removing bloodstains and bullet scars. The suspect was charged with seven counts of murder and three counts of attempted murder. He has not yet entered a plea.
Source: http://newsok.com/christian-college-resuming-classes-after-attack/article/feed/373713?custom_click=pod_headline_usnational-news

For more stories, see items **53** and **54**

[Return to top]

Emergency Services Sector

39. *April 24, States News Service* – (Massachusetts) **Former EMT instructor pleads guilty in Mass. EMT recertification fraud.** A former Emergency Medical Technician (EMT) instructor pleaded guilty in connection with submitting training records that falsely showed dozens of emergency personnel attended courses they were required to complete to maintain their certification, the Massachusetts attorney general announced April 24. The top four executives of a local ambulance company were also charged for their roles in the scheme. These co-defendants are the president/CEO, chief operating officer, and vice presidents, respectively, of LifeLine Ambulance in Woburn. The men are each charged with OEMS Violation [False Statements to OEMS/Evade OEMS Requirements] and Conspiracy to Commit OEMS Violation. In December 2008, the attorney general's office began the first phase of its investigation into fraudulent EMT re-certification. That investigation culminated with the indictments of the former police chief of the Hamilton Police Department (HPD); a former Wenham Police Department lieutenant and Ipswich selectman; the training coordinator for the Danvers-based Lyons Ambulance Service (Lyons), who is the retired fire chief of Middleton and Ipswich, and; a former reserve police office from HPD who conducted EMT training. The two instructors in that case have since pleaded guilty. The second phase of the attorney general's investigation resulted in the indictment of five people: one EMT instructor,

two paramedics, and two EMTs for their roles in a similar fraudulent scheme.
Source: http://www.emsworld.com/news/10704858/former-emt-instructor-pleads-guilty-in-mass-emt-recertification-fraud

40. *April 23, WLBZ 2 Bangor* – (Maine) **Emergency radios jammed in York County.** Maine's Lebanon Rescue Department is offering a $500 reward for information leading to the person who has been jamming their radios. The assistant chief said other departments have been affected too. He said the person sometimes blocks out radio traffic, or sometimes whistles into the radio, making it impossible for emergency crews to get their calls out. The interference has become more and more frequent, and the assistant chief said April 22 it went to a new level when the person actually blocked him from radioing for advanced life support for a patient. Lebanon rescue is now working with the Federal Communications Commission to see if the person's radio signal can be traced.
Source: http://www.wlbz2.com/news/article/198838/3/Emergency-radios-jammed-in-York-County

41. *April 23, KOVR 13 Sacramento* – (California) **Rocklin Police receiving disruptive communication over scanner.** In Rocklin, California, somebody has been jamming the Rocklin Police Department's scanner signal on a nightly basis since April 19, KOVR 13 Sacramento reported April 23. "This person will come on the air at various times," said a department spokesperson. "It's really disruptive." The person or people jamming the signal have refused to stop, despite being read a Federal Communications Commission warning. Rocklin police said they will have a hard time tracking down the culprit, and they apparently are the only area police department affected.
Source: http://sacramento.cbslocal.com/2012/04/23/rocklin-police-receiving-disruptive-communication-over-scanner/

For more stories, see items **4**, **14**, **51**, **52**, **53**, **54**, **57**, and **59**

[Return to top]

Information Technology Sector

42. *April 24, Softpedia* – (International) **Microsoft Office flaw exploited in the wild with malicious documents.** Security researchers from McAfee warn the CVE-2012-0158 vulnerability that exists in Microsoft Office and other products that use MSCOMCTL.OCX is being exploited in the wild with the aid of maliciously crafted RTF, Word, and Excel files. The security hole was patched with the April 2012 updates, but many users failed to apply them, giving cybercriminals the opportunity to launch malicious operations. Experts found the specially designed files come with a vulnerable OLE object embedded, usually being served to users via unsolicited e-mails. When the malevolent file is opened, the victim sees a regular document presented as bait, but in the background, the a trojan is installed. The infection begins when the Word process opens the crafted document. The CVE-2012-0158 flaw is exploited and the shellcode in the OLE file is triggered. This shellcode is responsible for installing the trojan in the Temp folder. At this stage, the same shellcode starts a new Word process

and opens the bait document, which is also dropped in the same Temp directory. The first process is terminated and the victim is presented only with the legitimate-looking document. Because in the first step the malicious element is executed and only then the genuine file is run, users whose computers are targeted may see that Word opens, quits, and then, almost immediately, re-launches to display the bait.
Source: http://news.softpedia.com/news/Microsoft-Office-Flaw-Exploited-in-Wild-with-Malicious-Documents-266068.shtml

43. *April 24, The Register* – (IDG News Service) **Hackers now pick tools from script kiddies' toybox – report.** Hackers are increasingly turning to automated software tools to launch attacks. According to research from Imperva, more than 60 percent of SQL injection attacks and as many as 70 percent of Remote File Inclusion attacks (the two most common attack types) are automated. Remote File Inclusion attacks allows hackers to plant back doors on PHP-based Web sites. Tools like Havij and SQLMap are used by miscreants to probe for vulnerabilities and execute SQL injection attacks. These tools also employ techniques to evade detection, such as periodically changing headers or splitting attacks through controlled hosts to avoid black-listing. In the past, using attack tools was purely for novices but these attitudes are changing, said Imperva's director of security strategy. Automatic attack tools can be used to attack more applications and exploit more vulnerabilities than any manual method, making them a useful adjunct for skilled attackers.
Source: http://www.theregister.co.uk/2012/04/24/crackers_tools/

44. *April 24, IDG News Service* – (International) **India overtakes U.S. as top email spam source.** The volume of e-mail spam that originated from India during the first 3 months of 2012 exceeded the volume coming from the United States and transformed the Asian country into the world's top spam source, security firm Sophos said April 23. India was responsible for 9.3 percent of global e-mail spam traffic seen from January to March, according to Sophos' latest Dirty Dozen report, which lists the top 12 countries from which most spam originates. The United States, which has been the traditional leader of the list, came in second place after India during the first quarter of 2012, at 8.3 percent. It was followed by South Korea with 5.7. The vast majority of spam is sent by computers infected with some type of malware and are part of a botnet, a senior technology consultant at Sophos said. "If you have a spam in your inbox, there's an almost one in ten chance that it was relayed from an Indian computer."
Source:
http://www.computerworld.com/s/article/9226506/India_overtakes_U.S._as_top_email_spam_source?source=rss_security&utm_source=feedburner&utm_medium=feed&utm_campaign=Feed:+computerworld/s/feed/topic/17+(Computerworld+Security+News)&utm_content=Google+Reader

45. *April 24, IDG News Service* – (International) **Macs more likely to carry Windows malware than Mac malware, Sophos says.** One in 5 Mac computers is likely to carry Windows malware, but only 1 in 36 is likely to be infected with malware specifically designed for the Mac OS X, according to study performed by antivirus firm Sophos. Sophos collected malware detection statistics from 100,000 Mac computers that run its free antivirus product and found that 20 percent of them contained one or more types of

Windows malware. When stored on a Mac, Windows malware is inactive and cannot do any harm, unless that computer has Windows installed as a secondary OS. However, such malicious files can still be transferred unknowingly by Mac users to Windows machines via file sharing, USB memory sticks, external hard disk drives, and other removable media devices. Sophos' analysis also revealed that 2.7 percent of the 100,000 scanned Macs were actually infected with Mac OS X malware, and a large part of those infections, 75 percent, were with the Flashback trojan.
Source:
http://www.computerworld.com/s/article/9226517/Macs_more_likely_to_carry_Windows_malware_than_Mac_malware_Sophos_says?source=rss_security&utm_source=feedburner&utm_medium=feed&utm_campaign=Feed:+computerworld/s/feed/topic/17+(Computerworld+Security+News)&

46. *April 24, Softpedia* – (International) **TreasonSMS bug allows hackers to execute malicious code on iPhones.** Researchers from the Vulnerability Lab found high severity HTML Inject and File Include security holes in TreasonSMS, an iPhone application that allows users to send text messages from their desktop computers by turning the phone into a SMS Web server. According to the experts, the vulnerabilities can be exploited remotely, allowing an attacker to "include malicious persistent script codes on the application-side of the iPhone." The security hole can also be leveraged to inject Web shell scripts that would give cybercriminals complete control of the affected application directory. If the device is jailbroken, things become even more complicated. On tampered iPhones, an attacker could take control not only of the application folder, but also of the entire phone.
Source: http://news.softpedia.com/news/TreasonSMS-Bug-Allows-Hackers-to-Execute-Malicious-Code-on-iPhones-266214.shtml

47. *April 24, The Register* – (International) **Number-munching clouds are godsend for cybercrooks - experts.** Cloud computing providers recently came under fire from security experts who blamed them for giving cyber criminals the tools to launch attacks more easily, efficiently, and anonymously than ever before. Speaking at the fourth InfoSecurity Summit in Hong Kong April 24, a senior consultant at the city-state's computer emergency response team argued that crooks are making the most of the sudden rise of distributed number-crunching services. "They are using it more efficiently for Web hosting and they can subscribe to cloud services to get bandwidth on demand," he said. "They can hack computers thanks to the computing power of Amazon and it's very hard to trace them. We need to solve this problem with the cloud service providers."
Source:
http://www.theregister.co.uk/2012/04/24/infosecurity_blame_cloud_computing/

48. *April 23, eSecurity Planet* – (International) **Anonymous hackers dominate IT security pros' fears.** According to the 2012 Bit9 Cyber Security Research Report, 64 percent of IT security professionals believe their organizations will be targeted by cyberattacks within the next 6 months, and 61 percent say those attacks are most likely to be led by members of Anonymous or other hacktivists. However, the attack methods that dominate security pros' concerns are not tied to Anonymous. Forty-five percent of

respondents are most worried about malware attacks, and 17 percent are concerned about spear phishing (both common attack methods for cybercriminals and nation states), while Anonymous' favored method, the distributed denial-of-service attack, leads the concerns of only 11 percent of respondents.
Source: http://www.esecurityplanet.com/hackers/anonymous-hackers-dominate-it-security-pros-fears.html

49. *April 23, Threatpost* – (International) **Google ups bounty for bugs to $20,000.** Google said it is updating its rewards and rules for the bounty program, which is celebrating its first anniversary. In addition to a top prize of $20,000 for vulnerabilities that allow code to be executed on product systems, Google said it would pay $10,000 for SQL injection and equivalent vulnerabilities in its services, and for certain vulnerabilities that leak information or allow attackers to bypass authentication or authorization features. The company said it would also begin distinguishing between the prices paid for vulnerabilities in high risk applications — such as Google Wallet — and those in lower risk applications and products from what it terms "non integrated acquisitions."
Source: http://threatpost.com/en_us/blogs/google-ups-bounty-bugs-20000-042312

50. *April 23, ZDNet* – (International) **New Flashback variant silently infects Macs.** The Flashback trojan that infected more than 600,000 Apple Macs earlier in April still reportedly has a very high infection rate, despite the fact Apple patched the Java vulnerability and released a removal tool. Now, security firm Intego says it discovered a new Flashback variant that installs without prompting the user for a password. This version, which Intego refers to as Flashback.S, places its files in the user's home folder. Once Flashback.S is done installing itself, it then deletes all files and folders in ~/Library/Caches/Java/cache to hide remove the applet from the infected Mac. This is done to avoid detection or sample recovery, according to the security firm. Two other Mac-specific trojans were discovered since Flashback's hype: one that also exploits Java and another that exploits Microsoft Word.
Source: http://www.zdnet.com/blog/security/new-flashback-variant-silently-infects-macs/11686

For more stories, see items **2**, **10**, **13**, **15**, **16**, and **52**

Internet Alert Dashboard

To report cyber infrastructure incidents or to request information, please contact US-CERT at sos@us-cert.gov or visit their Web site: http://www.us-cert.gov

Information on IT information sharing and analysis can be found at the IT ISAC (Information Sharing and Analysis Center) Web site: https://www.it-isac.org

[Return to top]

Communications Sector

51. *April 24, WZZM 13 Grand Rapids* – (Michigan) **Dispatch phone problems easing.** Emergency dispatchers in Montcalm County, Michigan, reported problems

with cellular phone service in the Greenville area that may be linked to landline problems in Kent and Ionia counties, WZZM 13 Grand Rapids reported April 24. A fiber optic line cut in Kent County's Grattan Township caused the problems. Kent and Ionia County dispatchers have said their problems with landline service have been fixed.
Source: http://www.wzzm13.com/news/article/210422/2/Upate--Dispatchers-Phone-problems-in-3-counties

52. *April 24, KNSD 7 San Diego* – (California) **Thousands, not millions, of broadband lines interrupted in Alpine: Centurylink.** Broadband lines used by many customers in the San Diego area were down when a fiber optic cable was cut early April 24 officials said. Someone cut the connection between midnight and 1 a.m. in the rural community of Alpine east of San Diego. Seventy-five feet of fiber optic cable was taken along with 6 feet of 600 strand copper cable according to the San Diego County Sheriff's Department. An estimated 10 million broadband lines were down according to deputies. A crew was working April 24 to repair the bundle of copper lines that were compromised. Deputies said the Alpine Sheriff's Station and the Pine Valley Sheriff's Station were affected by the interruption of the broadband lines, however the incident did not interrupt 9-1-1 service. Just after midnight a representative for Century Link Fibertron received notification the lines were down, officials said. The fiber optic cable involved is considered the backbone of the company's nationwide network deputies said. A Centurylink spokeswoman said a man crawled into a manhole and cut into the network to try to steal the copper cable. She said thousands, not millions, of customers were affected by the outage, and she expected the network to be restored by 1 p.m. Pacific Time. Three cables were involved in the incident according to an AT&T spokeswoman. One cable was Centurylink's, she said. While some AT&T cell sites were affected by the attempted theft, crews were working to gauge how many customers were without service, she said.
Source: http://www.nbcsandiego.com/news/local/Broadband-Lines-Cut-Copper-Theft-Alpine-Defense-Dept-148669775.html

53. *April 23, Government Security News* – (National) **FCC adds VoIP and broadband providers to its disaster reporting system.** The U.S. Federal Communications Commission (FCC), which has already established a Disaster Information Reporting System (DIRS) to gather contact information from wireless, wireline, broadcast, cable, and satellite communications providers that might be useful during an emergency, has decided to expand the coverage of the DIRS to include Voice over Internet Protocol (VoIP), Internet Protocol, and broadband Internet Service Providers. The FCC decided to take this step because so many consumers, businesses, and government agencies have come to rely on broadband and VoIP services for their everyday and emergency communications, according to a Federal Register notice posted by the FCC April 23.
Source: http://www.gsnmagazine.com/node/26174?c=communications

For another story, see item **46**

[Return to top]

Commercial Facilities Sector

54. *April 24, Framingham MetroWest Daily News* – (Massachusetts) **Six-alarm fire in Marlborough leaves 67 homeless.** A 6-alarm fire ripped through the top floor of a condominium complex in Marlborough, Massachusetts, April 23, leaving 67 people temporarily homeless. Firefighters from a dozen communities battled the fire much of the day, drawing water from nearby Lake Williams to increase the volume they poured onto the fire. Four firefighters were sent to the hospital with minor injuries and were released, a fire chief said. The fire appeared to have started in the top floor of the building, which was where residents stored property. Most of the fire was confined to the top floor, but the building received extensive water damage. Traffic on Route 20 was rerouted throughout the day and into the evening. The exits leading to Marlborough from Interstate 495 were also closed. Power was shut down to the area for firefighter safety, which forced Marlborough District Court to shut down for the day.
Source: http://www.metrowestdailynews.com/news/x1780487469/3-alarm-fire-in-Marlborough

55. *April 23, NewsCore* – (International) **U.S. warns of terror attack targeting hotels in Kenya.** The U.S. Embassy in Nairobi, Kenya, warned April 23 it received "credible information" regarding an attack on hotels and government buildings in the Kenyan capital. "Timing of the attack is not known, however, the Embassy has reason to believe that the potential attack is in the last stages of planning. The U.S. Embassy urges Americans to remain aware of their surroundings and vigilant of their personal security," the message posted on the embassy's Web site stated. The message provided no further details on the nature of the threat.
Source: http://www.foxnews.com/world/2012/04/23/us-warns-terror-attack-targeting-hotels-in-kenya/

56. *April 23, KOIN 6 Portland* – (Oregon) **Blaze breaks out at SE Portland printing products manufacturer.** A fire at a Portland, Oregon printing products manufacturer April 23 forced the evacuation of nearby businesses and prompted a HAZMAT response. Magnesium shavings and plates made battling the fire difficult, according to Portland Fire and Rescue. A HAZMAT team was also called due to health hazards from the smoke emitted by the shavings. Crews used 15 sandbags from a nearby building supply business, along with combustible fire extinguishers, to finally contain the fire.
Source: http://www.koinlocal6.com/mostpopular/story/Blaze-breaks-out-at-SE-Portland-printing-products/iX7E3VQ_ek-g7LZ-2kBSYg.cspx

57. *April 23, Connecticut Post* – (Connecticut) **Former Conn. firefighter admits to setting string of fires.** A former volunteer firefighter turned serial arsonist faces up to 10 years in prison after pleading guilty April 20 to setting fires in Fairfield, Easton, and Monroe, Connecticut, that destroyed homes and businesses and caused hundreds of thousands of dollars in damage. The man pleaded guilty to six counts of second-degree arson, two counts of third-degree arson, three counts of first-degree criminal mischief, and one count of reckless burning. He had been charged with setting 11 fires between July and September 2011. Two Fairfield firefighters suffered minor injuries fighting

one of the fires.
Source: http://www.firehouse.com/news/10704450/former-conn-firefighter-admits-to-setting-string-of-fires

58. *April 21, WJZ 13 Baltimore* – (International) **Under Armour employees' personal information lost.** A data breach may have exposed Under Armour employees' names, Social Security numbers, and salary information, WJZ 13 Baltimore reported April 21. An unencrypted thumb drive containing information on employees of the Baltimore-headquartered company was lost in the U.S. mail on or about April 12 by its auditing firm, PWC. There was no evidence the employee information was compromised. Employees will receive free credit monitoring and identity protection for a year as a precaution.
Source: http://baltimore.cbslocal.com/2012/04/21/under-armour-employees-personal-information-lost/

For more stories, see items **8**, **17**, and **53**

[Return to top]

National Monuments and Icons Sector

59. *April 23, Associated Press* – (Colorado) **Changes recommended to Colorado wildfire response.** State officials recommended organizational changes to the Colorado State Forest Service following a deadly wildfire that grew out of a prescribed burn set by the agency. April 23, the governor announced a proposal to have the agency's wildfire management functions and the state division of emergency management report to the Colorado Department of Public Safety. The state forest service is currently part of Colorado State University (CSU) and reports to academic officials, not state emergency officials. The CSU president said forest research and management would stay under the umbrella of the university. Legislation is needed to enact the change. The governor said the transfer would be smooth and could be accomplished as early as the end of July. Embers from a controlled burn the state forest service set March 22 reignited in heavy winds, sparking a wildfire March 26 near Conifer that damaged at least 23 homes, and left 3 people dead. An April 16 review led by a veteran forest manager examining the controlled burn found firefighters departed from their plan on one point by patrolling the perimeter for only 2 consecutive days after it was ignited.
Source: http://www.gazette.com/news/response-137407-wildfire-changes.html

[Return to top]

Dams Sector

60. *April 24, Corning Leader* – (New York) **Flood control funds received for tri-county area.** The Corning Leader reported April 24 that the New York governor recently announced Chemung, Schuyler, and Steuben counties were awarded $4.25 million in New York Works funding to make improvements to flood-control infrastructure. Of the

funding, $2.7 million will be used for two projects in the City of Elmira and in the Corning-Painted Post area. For both projects, work will include inspecting and repairing conduits, levees, and floodwalls; upgrading closure structures; repairing banks; surveying; and repairing operators. Both projects are expected to begin soon, the New York Department of Environmental Conservation (DEC) said. The remaining $1.5 million will be distributed among several other municipalities. The DEC maintains 106 flood-control systems statewide, of which 91 have been rated as minimally acceptable or unacceptable by the U.S. Army Corps of Engineers.
Source: http://www.steubencourier.com/news_now/x787561262/Flood-control-funds-received-for-tri-county-area

61. *April 23, Williston Herald* – (North Dakota) **Corps approves $11.7 million for Williston levee.** The U.S. Army Corps of Engineers awarded $11.7 million in federal funding April 20 to repair and upgrade the levee that separates Williston, North Dakota, and the Missouri River. After heavy rains and record snowmelt in 2011, the levee was damaged as the Missouri reached a record flood stage. No major damage was reported in Williston, however, some lowing structures, roads, and oil wells flooded. "The project was designed to provide protection to the low lying areas of the city against backwater effects from Lake Sakakawea, the reservoir for Garrison Dam," according to a press release from the Corps. A portion of the money will go to restore the levee crest to an approximate elevation of 1,863 feet above sea level, and the levee will be seeded for grass.
Source: http://www.willistonherald.com/news/corps-approves-million-for-williston-levee/article_572b9408-8d6b-11e1-aa28-0019bb2963f4.html

[Return to top]

Department of Homeland Security (DHS)
DHS Daily Open Source Infrastructure Report Contact Information

About the reports - The DHS Daily Open Source Infrastructure Report is a daily [Monday through Friday] summary of open-source published information concerning significant critical infrastructure issues. The DHS Daily Open Source Infrastructure Report is archived for ten days on the Department of Homeland Security Web site: http://www.dhs.gov/IPDailyReport

Contact Information

Content and Suggestions:	Send mail to cikr.productfeedback@hq.dhs.gov or contact the DHS Daily Report Team at (703)387-2267
Subscribe to the Distribution List:	Visit the DHS Daily Open Source Infrastructure Report and follow instructions to Get e-mail updates when this information changes.
Removal from Distribution List:	Send mail to support@govdelivery.com.

Contact DHS

To report physical infrastructure incidents or to request information, please contact the National Infrastructure Coordinating Center at nicc@dhs.gov or (202) 282-9201.
To report cyber infrastructure incidents or to request information, please contact US-CERT at soc@us-cert.gov or visit their Web page at www.us-cert.gov.

Department of Homeland Security Disclaimer